Novel NeoFuse Based Random Number Seed Generator

eMemory

ABSTRACT

eMemory, as the leading company providing logic-NVM technologies, has long-term partnership with TSMC since 2002. To fulfill the needs of logic NVM from mature to leading-edge technology nodes for various applications in IoT, eMemory offers NeoFuse anti-fuse technology which utilizes core device as memory cell element and extends the logic NVM solution to follow Moore's law.

Along with TSMC 9000 IP compliance quality control, eMemory robust design capability and excellent customer engineering quality, eMemory NeoFuse technology is well recognized by customers and spread out quickly from 0.11um/ 65nm/55nm/40nm/28nm/16nm to 10nm/7nm and covers logic, LP/ULP, HV, CIS, HPM/HPC, FFP/FFC platforms. Widely used in the code storage, identification, analog trimming, and encryption/ security protection applications.

Beside the stunning achievement of being the first vendor to provide qualified 16nm FinFET Plus/Compact process OTP IP in the world, eMemory also committed to do technical innovations. Here we are glad to share the world first NVM random number seed for PUF, Physical Unclonable Function, and encryption applications.

As a logic NVM expert, eMemory utilize and magnify the memory cells tiny differences from uncontrollable physical processes randomness to create the world first unique NVM random number seed. Compared to standard SRAM or oscillator based random number seed, there is no data unstable issue at extreme operation conditions like high/low temperature, high/low Vdd environment. That could save lots of the effort for error correcting design.

Combine with security protection functions, innovation circuit design and non-volatile advantages, the NeoFuse random number seed is truly random, extremely stable within all corner conditions, and in-visible while under invasive or non-invasive attacks. And undoubtedly, this unique silicon finger print function and be easily adopted into all qualified NeoFuse platforms.

In a short summary, eMemory is going to present the advantages and roadmap of NeoFuse technology in TSMC advance nodes. And the world first NVM random number seed would also be introduced in this meeting.

Novel NeoFuse Based Random Number Seed Generator

Sean Wang
eMemory Technology Inc.
Sep. 2016

IPR Notice

Outlines

- About eMemory
- Trustworthy NeoFuse Technology
- Novel NeoFuse Based Random Number Seed Generator
- Summary

Corporate Overview

Patent
353+ Patents Issued
190+ Pending

Support
228+ Employees with
161+ NVM IP Developers

Experience
1096+ Verified NVM IP
3344+ Cumulative NTO
13M+ Wafers Shipped

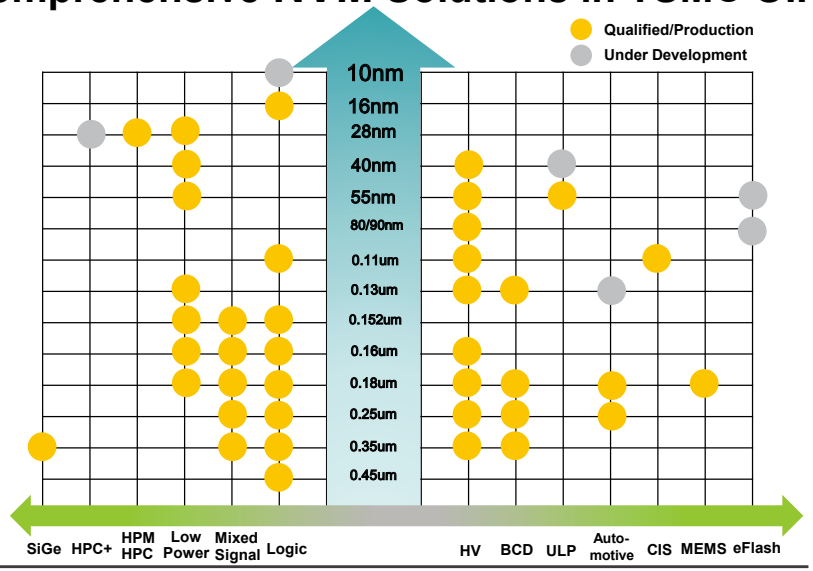
Award
Consecutive 6-year Awarded
TSMC Best IP Partners

Trustworthy Logic NVM

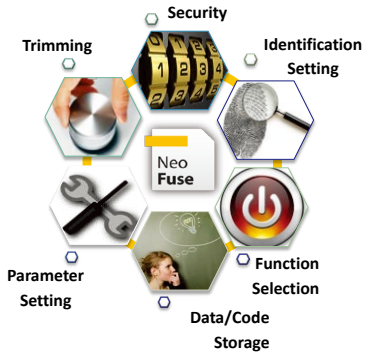
- Completed Logic NVM **lineup** offer one-stop-shop solution.
  - Compatible to any process
  - Robust structure
  - Low process cost
  - Competitive macro sizes
  - Easy integration
  - Easy porting

eMemory NVM Technology	OTP		MTP	
	Neo Fuse	Neo Bit	Neo MTP	Neo EE
Product Type	OTP	OTP	MTP	EEPROM
Endurance (Cycles)	10	10	1K~10K	10K~100K
Additional Mask Steps	0	0	0	0
Technology	Anti-Fuse	Floating gate	Floating gate	Floating gate
Scalability	Simple	Simple	Simple	Simple
Memory Density	< 4Mb	HD < 512Kb GHD < 16Mb	< 512Kb	< 4Kb
Testability	No	Yes	Yes	Yes

Comprehensive NVM Solutions in TSMC OIP



OTP Demand and NeoFuse Strengths



- Larger NVM density for increasing functions
  - NeoFuse has good competitiveness with superior IP characters and area.
- Low power operation
  - Lower to 1.62V operation @ 40nm/55nm nodes for energy sensitive applications.
- Vulnerability is getting more attention
  - Comprehensive secure protection functions to against varied attacks.

NeoFuse Security Protection Features

Invasive Attacks	• Reverse engineering: intrinsically invisible / scrambling
	• Microprobing: shielding / layout / scrambling / fake output / fault detection
	• Circuit edit: metal shielding / security-oriented layout
	• VC inspection: intrinsically invisible / layout / scrambling
Semi-Invasive Attacks	• Optical fault injection: shielding / layout / fake output / fault detection
	• Backside imaging: intrinsically invisible / scrambling / SA cover-up
	• UV erasure & magnetic attack: intrinsically unalterable
Non-Invasive Attacks	• Timing & power analysis: bit lock scheme / SA cover-up
	• EM emanation: metal shielding
	• Power glitching: power detection / built-in CP
	• Data tampering: bit lock scheme

Certified by several third-party CAs

Low Power Operation IP

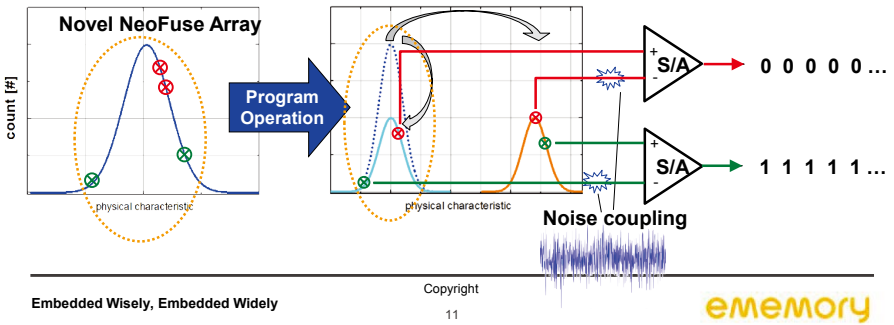
- **Target for low power environment like wireless sensor network and other portable devices. Can be used for application code storage, like Bluetooth Smart profiles, or keep the system configuration and calibration data.**

Technology Node		40nm LP(1.1V/2.5V) 40nm ULP (0.9V/2.5V)		55nm LP(1.2V/2.5V) 55nm ULP (0.9V/2.5V)	
Read Voltage	VDD	0.81V~1.21V	0.81V~1.21V	0.81V~1.32V	0.81V~1.32V
	VDD2	1.62V~3.6V	2.25V~3.6V	1.62V~3.6V	2.25V~3.6V
Access Time (max)		50ns	50ns	50ns	50ns

Novel NeoFuse Based Random Number Seed Generator

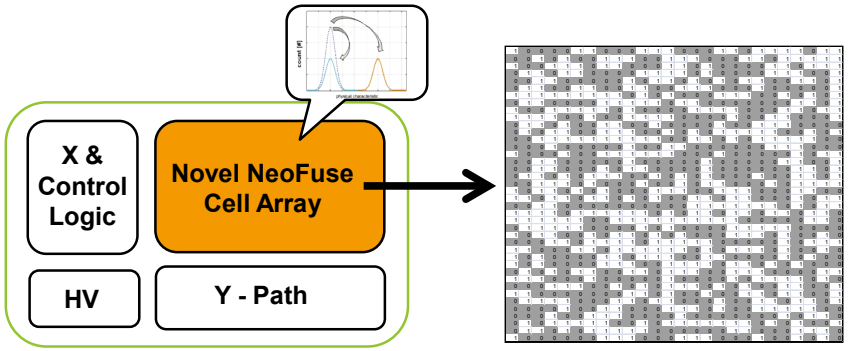
NeoFuse Random Number Seed

- **Through innovative NeoFuse cell design, we can obtain random bits with wide noise margin as NeoFuse OTP by simply performing program operation**
  - **Achieved by inherent self-feedback mechanism**
  - **No complicated circuitry, like median-detection, is required**



Random Number Seed Generator

- **After performing program operation (to induce oxide rupture) on the novel NeoFuse array, a true random number seed is generated automatically.**

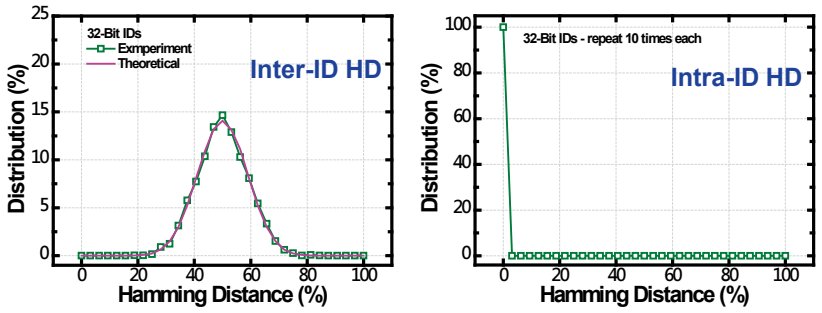


Competitive Comparison

Key Feature	Arbiter / RO / FF	SRAM	NeoFuse
(Uniqueness & randomness) Entropy Source	Propagation delay mismatch	Composition transistor mismatch	Random oxide weak spot from process variation
(Reliability) Data robustness	Need complicate ECC due to aging and environment (temp. or voltage sensitive)	Need complicate ECC due to aging and environment (temp. or voltage sensitive)	No need for ECC with robust Neofuse structure in all operation corners.
(Unclonability) Attack immunity	Data removed by power failure	Data removed by power failure	Intrinsically invisible
Application & implementation	MUX/RO/FF array as random source with security/protection design. Need extra NVM to store helper data or use battery backup	SRAM array as random source with security/protection design. Need extra NVM to store helper data or use battery backup	NeoFuse array as random number seed with security / protection design. Encryption storage in built-in NeoFuse OTP

Code Randomness Verification

- Extracted random numbers are divided into 32-bit sub blocks.
- Inter-ID hamming distance shows perfect uniqueness (peak at 50% distance)
- Intra-ID HD shows perfect consistency for 10-time repeats



Code Randomness Verification

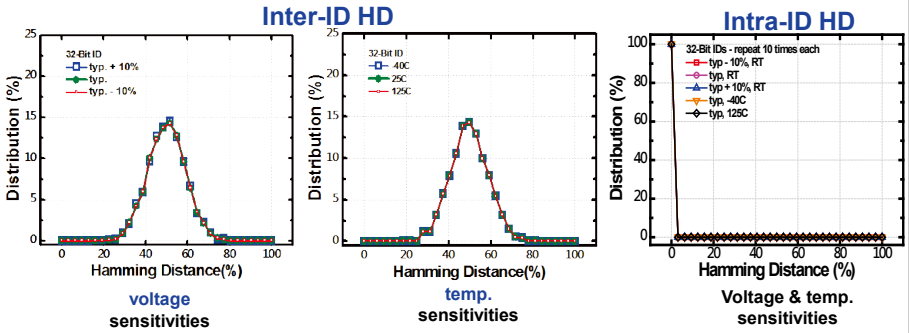
- Use NIST 800-22 test suite for randomness analysis
- **PASS** all test items fit for current data size

tested random number: (bitmap1) **3300-bit** bit string, one sequence(bit string)

#	Statistical Test	Recommended n (length of bit string)	P-value	P/F (P > 0.01?)
1	Frequency	>100	0.916815	P
2	Block Frequency (m=128)	>100	0.444974	P
3	Cusum-Forward	>100	0.814082	P
4	Cusum-Reverse	>100	0.844535	P
5	Runs	>100	0.554068	P
6	Longest Runs of Ones (M=8)	>128	0.986013	P
7	Binary Matrix Rank (M=Q=32)	>38912	0.333851	skip
8	Spectral DFT	>1000	0.689627	P
9	Non-overlapping Templates (m=9, B=000000001)	?	0.766487	P
10	Overlapping Templates (m=9, B=111111111)	>1E6	0.830234	skip
11	Universal	>387840	NA	skip
12	Approximate Entropy (m=5)	m < (log2 n) - 5	0.337266	P
13	Random Excursions (x=+1)	>1E6	NA	skip
14	Random Excursions Variant (x=-1)	>1E6	NA	skip
15	Linear Complexity (M=500)	>1E6	0.96977	skip
16	Serial (m=8)	m < (log2 n) - 2	0.169443 0.122184	P

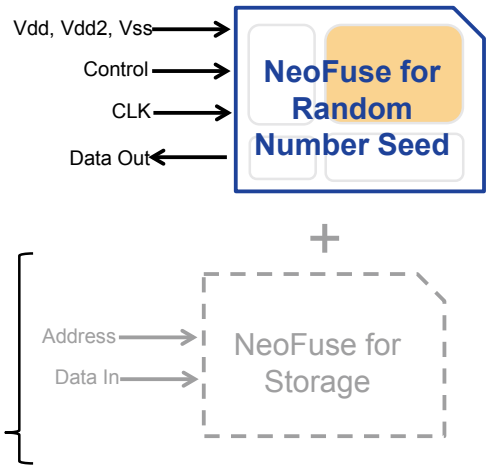
Code Robustness Verification

- Excellent random number seed robustness for fully operation ranged temperature (-40~125˚C) and voltage (typical V_{DD} +/- 10%) .



Random Number Seed Generator

Key Feature
• 55nm ULP(+eFlash) Process
• VDD/VDD2 Dual Power Supply
• Built-in Charge Pump
• RNS Operation Modes: − Random Number Seed Enrollment − BIST for Random Number Seed Margin Verification − Random Number Seed Burst Read (flexible, up to 64Kb)
• Security Protection Features: − Power Detection − Metal Shielding − True Random Scrambling − S/A cover-up − Data fault injection detection
• (Optional) OTP Storage up to 256Kb



Summary

- NeoFuse meet TSMC IP9000 quality compliance and reach low-power, high-yield, high-reliability, secure protected requirements for various applications.
- Random number seed with wide noise margin is generated from innovative NeoFuse array with simple self-feedback mechanism in program operation.
- Data uniqueness and randomness are verified by inter-/intra-ID hamming distance and NIST 800-22 test suite respectively.
- Data robustness is verified with corner operation conditions including full voltage range at high/low temperature without extra error code correcting circuitry help.

ememory

Embedded Wisely, Embedded Widely